



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/652,454	08/31/2000	David Cheriton	CISCP537	3379
26541	7590	03/10/2004	EXAMINER	
RITTER, LANG & KAPLAN 12930 SARATOGA AE. SUITE D1 SARATOGA, CA 95070			SIMITOSKI, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 03/10/2004

6

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/652,454

Applicant(s)

CHERITON, DAVID

Examiner

Michael J Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 August 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 August 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 5.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. The IDS of 1/21/2003 has been received and considered.
2. Claims 1-22 are pending.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 2 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claim is indefinite because "reducing the amount of packets that are filtered" is contradictory, because all packets are filtered (subject to filtering criteria) upon coming into a firewall. "Filtered out" might be a more proper term.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, 3-6, 8-10, 12-13 & 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,598,034 to Kloth in view of "Router Plugins: A Software Architecture for Next Generation Routers" by Decasper et al. (Decasper).

Regarding claims 1 & 22, Kloth discloses analyzing data from a network (col. 3 lines 61-67 & col. 4 lines 1-13), detecting potentially harmful traffic (bit patterns indicative of intrusion) (col. 3 lines 15-39), and generating filters to prevent harmful network flows from passing (intrusion protection) (col. 4 lines 38-67 & col. 5 lines 1-18). Kloth further states that the analysis and rules application is applied to the entire IP flow and that incoming data is classified, but does not explicitly disclose separating the data into different network flows. However, Decasper teaches separating/classifying the data/packets into different network flows and applying policies to the flows (page 230 ¶3) to achieve enhance routing with benefits of low cost and fast lookups (page 240 ¶1-3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to separate the data into different network flows. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefits of low cost and fast lookups, as taught by Decasper (page 230 ¶3 & page 240 ¶1-3).

Regarding claims 3 & 4, Kloth discloses classifying packets based on a source device (col. 7 lines 29-55).

Regarding claim 5, Kloth discloses a system, as modified above, but lacks performing a lookup in a flow cache. However, Decasper teaches that using a flow table/flow cache allows for very fast lookup times for arriving packets (page 233 ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to perform a lookup in a flow cache. One of ordinary skill in the art would have been motivated to perform such a modification to achieve very fast lookup times for arriving packets, as taught by Decasper (page 233 ¶2).

Regarding claim 6, Kloth discloses analyzing statistics associated with a network flow (col. 11 lines 63-67 & col. 12 lines 1-16).

Regarding claim 8, Kloth discloses analyzing data in software (col. 13 lines 41-60) and Decasper teaches that software drivers for custom hardware can be used to achieve high-performance processing (page 231 §3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use custom hardware. One of ordinary skill in the art would have been motivated to perform such a modification to achieve high-performance processing, as taught by Decasper (page 231 §3).

Regarding claim 9, Kloth discloses a flow analyzer/router performing analysis on incoming packets (Fig. 7, col. 9 lines 50-67 & col. 10 lines 1-12).

Regarding claim 10, Kloth discloses the flow analyzer/router comprising software/parser (col. 9 lines 25-50).

Regarding claims 12 & 13, Kloth discloses analyzing traffic for overload conditions/denial of service attacks (col. 12 lines 1-16).

7. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kloth in view of Decasper, as applied to claim 1 above, in further view of U.S. Patent 6,389,352 to Gupta et al. (Gupta). Kloth discloses a system, as modified above, but lacks explicitly identifying a source address associated with a harmful network flow and generating a filter to prevent packets from that source from passing through the network. However, Gupta teaches that a router can filter packets when a predetermined router limit, such as a rate at which a router may receive packets from a particular source, has been exceeded, to prevent denial of service attacks (col. 7 lines 28-

Art Unit: 2134

52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to identify a source of a harmful packet flow and generate a filter to prevent incoming packets from the source. One of ordinary skill in the art would have been motivated to perform such a modification to prevent denial of service attacks, as taught by Gupta (col. 7 lines 28-52).

8. Claims 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kloth in view of Gupta.

Regarding claim 15, Kloth teaches analyzing network flows to detect harmful flows (col. 3 lines 15-67 & col. 4 lines 1-13). Kloth does not teach automatically generating a filter to prevent packets corresponding to the detected potentially harmful network flows from passing through the network device. However, Gupta teaches that to prevent denial of service attacks, it is required of a network device to determine harmful flows/exceeding router limit and discard packets from that flow (col. 7 lines 28-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to automatically generate a filter. One of ordinary skill in the art would have been motivated to perform such a modification to prevent denial of service attacks, as taught by Gupta (col. 7 lines 28-52).

Regarding claim 16, Kloth discloses a system memory (Fig. 6).

9. Claims 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kloth in view of Decasper in further view of U.S. Patent 6,453,345 to Trcka et al. (Trcka).

Regarding claim 18, Kloth discloses a netflow device/router operable to received streams/flows of packets (Fig. 7), a flow analyzer/parser operable to analyze the incoming flows and identify harmful flows (col. 3 lines 15-67 & col. 4 lines 1-13), and a filter generator/router operable to generate a filter to prevent packets corresponding to a harmful flow from passing through the network device (intrusion protection) (col. 4 lines 38-67 & col. 5 lines 1-18). Kloth lacks separating the streams/flows and creating a summary record containing information about the streams. However, Decasper teaches separating/classifying the data/packets into different network flows and applying policies to the flows (page 230 ¶3) to achieve enhance routing with benefits of low cost and fast lookups (page 240 ¶1-3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to separate the data into different network flows. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefits of low cost and fast lookups, as taught by Decasper (page 230 ¶3 & page 240 ¶1-3). Kloth, as modified above, lacks creating a summary record containing information about the flows. However, Trcka teaches a system that records network traffic data/record summaries to be analyzed later (col. 2 lines 10-65) to overcome the limitation that firewalls generally only protect against known types of security attacks and to detect virus patterns in transmitted data (col. 1 lines 53-67 & col. 2 lines 1-8). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to create a summary record containing information on a stream, as taught by Trcka, for each of the separated streams, as taught by Decasper. One of ordinary skill in the art would have been motivated to perform such a modification to detect viruses and detect attacks not previously known, as taught by Trcka (col. 1 lines 53-67 & col. 2 lines 1-65).

Regarding claim 19, Kloth discloses analyzing data in software (col. 13 lines 41-60) and Decasper teaches that software drivers for custom hardware can be used to achieve high-performance processing (page 231 §3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use custom hardware. One of ordinary skill in the art would have been motivated to perform such a modification to achieve high-performance processing, as taught by Decasper (page 231 §3).

Regarding claim 20, Kloth discloses a system, as modified above, but lacks an ACL classifier, a lookup device and a plurality of flow buckets. However, Decasper teaches separating/classifying the data/packets into different network flows and applying policies to the flows (page 230 ¶3) to achieve enhance routing with benefits of low cost and fast lookups (page 240 ¶1-3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to separate the data into different network flows using an ACL classifier. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefits of low cost and fast lookups, as taught by Decasper (page 230 ¶3 & page 240 ¶1-3). Further, Decasper teaches that using a flow table/flow cache allows for very fast lookup times for arriving packets (page 233 ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to perform a lookup in a flow cache using a lookup device. One of ordinary skill in the art would have been motivated to perform such a modification to achieve very fast lookup times for arriving packets, as taught by Decasper (page 233 ¶2). Further, Trcka teaches a system that records network traffic data/record summaries to be analyzed later (col. 2 lines 10-65) to overcome the limitation that firewalls generally only protect against known types of security attacks and to detect virus patterns in

Art Unit: 2134

transmitted data (col. 1 lines 53-67 & col. 2 lines 1-8). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include buckets containing information on particular flow, as taught by Trcka, for each of the separated streams, as taught by Decasper. One of ordinary skill in the art would have been motivated to perform such a modification to detect viruses and detect attacks not previously known, as taught by Trcka (col. 1 lines 53-67 & col. 2 lines 1-65).

10. Claims 7 & 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kloth in view of Decasper, as applied to claim 1 above, in further view of U.S. Patent 6,496,935 to Fink et al. (Fink).

Regarding claim 7, Kloth discloses a system, as modified above, but lacks propagating the generated filter to an upstream network device. However, Fink teaches that adding a pre-filtering module between a source and a firewall, rapid packet filtration can be achieved (col. 2 lines 1-40). The pre-filtering module is in communication with the firewall and receives instructions from the firewall regarding rules set by the firewall, so the pre-filtering module can filter the data stream (col. 2 lines 58-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to propagate the generated filter to an upstream network device, such as a pre-filtering module. One of ordinary skill in the art would have been motivated to perform such a modification to achieve rapid packet filtration, as taught by Fink (col. 2).

Regarding claim 11, Kloth discloses a system, as modified above, but lacks explicitly disclosing selecting a class of said network flows to analyze based on previously analyzed flows.

Art Unit: 2134

However, Fink teaches that adding a pre-filtering module between a source and a firewall, rapid packet filtration can be achieved (col. 2 lines 1-40). The pre-filtering module is in communication with the firewall and receives instructions from the firewall regarding rules set by the firewall, so the pre-filtering module can filter the data stream (col. 2 lines 58-67). The hardware-accelerated pre-filter module filters packets from flows already permitted/denied by the firewall, and therefore the firewall only analyzes flows from flows not previously analyzed (col. 2 lines 44-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a pre-filtering module and hence select flows to analyze based on previously analyzed flows. One of ordinary skill in the art would have been motivated to perform such a modification to achieve rapid packet filtration, as taught by Fink (col. 2).

11. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kloth in view of Gupta, as applied to claim 15 above, in further view of Fink. Kloth discloses a system, as modified above, but lacks propagating the generated filter to an upstream network device. However, Fink teaches that adding a pre-filtering module between a source and a firewall, rapid packet filtration can be achieved (col. 2 lines 1-40). The pre-filtering module is in communication with the firewall and receives instructions from the firewall regarding rules set by the firewall, so the pre-filtering module can filter the data stream (col. 2 lines 58-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to propagate the generated filter to an upstream network device, such as a

Art Unit: 2134

pre-filtering module. One of ordinary skill in the art would have been motivated to perform such a modification to achieve rapid packet filtration, as taught by Fink (col. 2).

12. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kloth in view of Decasper and Trcka, as applied to claim 18 above, in further view of Fink. Kloth discloses a system, as modified above, but lacks sending information on the filters to an upstream device and requesting the device to create a corresponding filter. However, Fink teaches that adding a pre-filtering module between a source and a firewall, rapid packet filtration can be achieved (col. 2 lines 1-40). The pre-filtering module is in communication with the firewall and receives instructions from the firewall regarding rules set by the firewall, so the pre-filtering module can filter the data stream (col. 2 lines 58-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to propagate the generated filter to an upstream network device, such as a pre-filtering module. One of ordinary skill in the art would have been motivated to perform such a modification to achieve rapid packet filtration, as taught by Fink (col. 2).

13. Claim 2, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over Kloth in view of Decasper, as applied to claim 1 above, in further view of "Application Note 2037 Nemesis Firewall" by Allied Telesyn. Kloth discloses a system, as modified above, but lacks refining rules to reduce the number of packets filtered. However, Allied Telesyn teaches that it is known in the art to refine the security policy/rules in a firewall because the default options are not specific (page 4, § Rules and Policies). Therefore, it would have been

Art Unit: 2134

obvious to one having ordinary skill in the art at the time the invention was made to refine the rules/policies. One of ordinary skill in the art would have been motivated to perform such a modification to personalize the filtering rather than using the defaults of a firewall/packet filter, as taught by Allied Telesyn (page 4, § Rules and Policies).

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. The NPL reference by Apisdorf was cited for teaching flow-based statistics collection and analysis.
- b. The NPL references by Gupta, Ilvesmaki, Lakshman & Newman were cited for teaching flow-based packet classification and routing/filtering/queuing/forwarding based on those flows.
- c. The NPL reference by Deering was cited for teaching the Ipv6 specification that contains packet header information concerning a flow ID used for specialized routing.
- d. The NPL reference by Cyberplaces was cited for also teaching refining firewall rules and reviewing logs as standard practice in the firewall/packet filter art.
- e. The '015, '775, '667, '012 & '150 references were cited for teaching general procedures and knowledge in the art of applying and/or generating rules/policies to/for packets/packet flows and for teaching common practices in firewall/packet filter designs.

Art Unit: 2134

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191.

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:

(703)746-7239 (for formal communications intended for entry)

Or:

(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Application/Control Number: 09/652,454

Page 13

Art Unit: 2134

MJS

March 2, 2004

A handwritten signature in black ink, appearing to be 'MJS', located below the 'Art Unit: 2134' text.A handwritten signature in black ink, appearing to be 'Norman M. Wright', located above the printed name.

NORMAN M. WRIGHT
PRIMARY EXAMINER